NetIQ® Identity Manager
Administrator’s Guide to Configure Auditing

October 2019
Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Copyright (C) 2019 NetIQ Corporation. All rights reserved.
## Contents

About this Book and the Library  
About NetIQ Corporation  

1 Overview  
   Identity Manager Auditing Architecture  
   Audit Format Type  
   Enabling Auditing  
   Considerations for Migrating to CEF  

2 Configuring NetIQ Sentinel with Identity Manager  

3 Installing and Configuring the Sentinel Collectors  
   Installing and Configuring the Universal CEF Collector  
   Installing and Configuring the SSPR Collectors  

4 Installing the Syslog Connector  
   Installing and Configuring the Syslog Connector  

5 Configuring Identity Manager Components to Log Audit Events in CEF Format  
   Advantages of CEF  
   Setting up CEF Configuration  
      Configuring Identity Manager Engine  
      Configuring Remote Loader  
      Configuring .NET Remote Loader  
      Configuring Java Remote Loader  
      Configuring Fanout Agent  
      Configuring Identity Applications  
      Configuring Identity Reporting  
      Configuring Data Collection Services  
      Configuring One SSO Provider  
      Configuring Self Service Password Reset  

6 Securing the Logging System  
   Enabling SSL Connection for User Application  
   Enabling SSL Connection for Identity Manager Engine  

7 Managing Identity Manager Events  
   Selecting Events to Log  
      Selecting Events for the User Application  
      Selecting Events for the Driver Set  
      Selecting Events for a Specific Driver  

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this Book and the Library</td>
<td>5</td>
</tr>
<tr>
<td>About NetIQ Corporation</td>
<td>7</td>
</tr>
<tr>
<td>1 Overview</td>
<td>9</td>
</tr>
<tr>
<td>2 Configuring NetIQ Sentinel with Identity Manager</td>
<td>13</td>
</tr>
<tr>
<td>3 Installing and Configuring the Sentinel Collectors</td>
<td>15</td>
</tr>
<tr>
<td>4 Installing the Syslog Connector</td>
<td>17</td>
</tr>
<tr>
<td>5 Configuring Identity Manager Components to Log Audit Events in CEF Format</td>
<td>19</td>
</tr>
<tr>
<td>6 Securing the Logging System</td>
<td>29</td>
</tr>
<tr>
<td>7 Managing Identity Manager Events</td>
<td>31</td>
</tr>
</tbody>
</table>
8 Using Status Logs .................................................................37
  Setting the Log Level and Maximum Log Size ..........................37
  Setting the Log Level and Log Size for the Driver Set .................37
  Setting the Log Level and Log Size for the Driver .......................38
  Viewing Status Logs .................................................................39
  Accessing the Driver Set Status Log ...........................................39
  Accessing the Publisher Channel and Subscriber Channel Status Logs .........................................................40

A Identity Manager Events ........................................................41
  Event Structure ...........................................................................41
  Remote Loader Events ...............................................................41
  Engine Events ............................................................................42
  Fanout Agent Events .................................................................45
  Identity Applications Events .......................................................45
  Identity Reporting Events ..........................................................50
  DCS Events ..................................................................................50

B Understanding the Properties Files for CEF Auditing ................53
  Understanding the auditlogconfig.properties File .........................53
  Identity Manager Engine, Remote Loader, and .NET Remote Loader .................................................................53
  Java Remote Loader and Fanout Agent ..........................................57
  Understanding the idmuserapp_logging.xml File .........................58
  Understanding the workflow_logging.xml File ............................61
  Understanding the idmrptdcs_logging.xml File ............................62
  Understanding the idmrptcore_logging.xml File ............................64

9 Troubleshooting .................................................................67
  Error on Identity Manager Dashboard Login Page .........................67
About this Book and the Library

The Identity Manager - Administrator’s Guide to Configure Auditing provides the information necessary to set up Identity Manager components for auditing events. You can then integrate NetIQ Sentinel with Identity Manager to provide auditing and reporting services.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

For more information about the library for Identity Manager, see the Identity Manager documentation website.
About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That’s the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that’s so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management
Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide: www.netiq.com/about_netiq/officelocations.asp
United States and Canada: 1-888-323-6768
Email: info@netiq.com
Web Site: www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide: www.netiq.com/support/contactinfo.asp
North and South America: 1-713-418-5555
Europe, Middle East, and Africa: +353 (0) 91-782 677
Email: support@netiq.com
Web Site: www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click Add Comment at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.
This guide helps you in implementing a uniform auditing across Identity Manager.

### Identity Manager Auditing Architecture

This section explains how different components work together to provide a uniform auditing infrastructure in Identity Manager.

Identity Manager provides event forwarding capabilities to Security Event Log Management solutions such as Sentinel and ArcSight. Sentinel is the preferred audit event destination for Identity Manager. The following diagram illustrates how Identity Manager is configured with Sentinel Event Source Management (ESM).

*Figure 1-1  Auditing through CEF*

1. An Identity Manager event occurs and it is sent to the logging services.
2. (Conditional) If the logging services cannot connect to the Sentinel Server, the events are stored in cache until the connection is reestablished.
3. The logging services sends the events to the Sentinel Server, which stores the events in the audit queue.
4. The events in the audit queue are sent to the Syslog Connector.
5. The Syslog Connector sends the events to the Universal CEF Collector, which parses the information and then stores the parsed events in the data store.

6. (Optional) The stored events can be used for reports.

Audit Format Type

**IMPORTANT:** Auditing with NAudit and XDAS for the Identity Manager components is discontinued from Identity Manager 4.8. If you were using XDAS and NAudit with any previous version of Identity Manager, you must use only CEF for auditing purposes going forward.

Previous versions of Identity Manager used a combination of different auditing solutions. Identity Manager now supports Common Event Format (CEF) to provide a uniform auditing solution across all Identity Manager components.

The following table lists the availability of CEF in each Identity Manager version.

<table>
<thead>
<tr>
<th>Identity Manager Version</th>
<th>Sentinel Collector Supported</th>
<th>Availability of Common Event Format (CEF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.6.x, where x is 0 to 4</td>
<td>NA</td>
<td>No</td>
</tr>
<tr>
<td>4.7 and 4.7.1</td>
<td>NetIQ Identity Manager collector</td>
<td>Yes</td>
</tr>
<tr>
<td>4.7.2 onward</td>
<td>Universal Common Event Format collector</td>
<td>Yes</td>
</tr>
<tr>
<td>4.8</td>
<td>Universal Common Event Format collector</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Enabling Auditing

Auditing is not enabled by default. You must enable it after you have installed the Identity Manager components. NetIQ provides different auditing options for Identity Manager components as listed in the following table:

<table>
<thead>
<tr>
<th>Component</th>
<th>Auditing Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Manager Engine, Remote Loader, Fanout Agent, Identity Applications, OSP, Identity Reporting, and Data Collection Services</td>
<td>To enable CEF auditing for these components, see “Setting up CEF Configuration” on page 19.</td>
</tr>
<tr>
<td>Identity Vault</td>
<td>To enable CEF auditing for Identity Vault, see Auditing with CEF in the NetIQ eDirectory Administration Guide</td>
</tr>
<tr>
<td>SSPR</td>
<td>To enable CEF auditing for SSPR, see Auditing for Self-Service Password Reset in the Self Service Password Reset Administration Guide.</td>
</tr>
</tbody>
</table>
Considerations for Migrating to CEF

To begin with the migration, you must first review the following considerations:

- Your current Identity Manager version.
- Your existing auditing configuration, that is, whether auditing is enabled or disabled.

**NOTE:** Auditing with NAudit and XDAS is discontinued from Identity Manager 4.8 release. If your auditing format type is not configured as CEF, then you may lose the audit events during migration to CEF format in Identity Manager 4.8.

The following table provides procedures to help you with the migration to CEF format. Select the procedure from this list depending on your current Identity Manager version and the existing auditing configuration.

<table>
<thead>
<tr>
<th>Current Identity Manager Version</th>
<th>Existing Auditing Configuration</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.6.x, where x is 0 to 4</td>
<td>NA</td>
<td>None</td>
</tr>
</tbody>
</table>

1. Install and configure the NetIQ Sentinel Universal CEF Collector. For more information, see “Installing and Configuring the Universal CEF Collector” on page 15.

2. Configure Identity Manager components to use Common Event Format (CEF). For more information, see “Configuring Identity Manager Components to Log Audit Events in CEF Format” on page 19.
<table>
<thead>
<tr>
<th>Current Identity Manager Version</th>
<th>Existing Auditing Configuration</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Pre-Upgrade Steps</td>
</tr>
<tr>
<td>4.7.x, where x is 0 to 4</td>
<td>If CEF auditing is disabled.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.7.x, where x is 0 and 1</td>
<td>If CEF auditing is enabled.</td>
<td>Install and configure the NetIQ Sentinel Universal CEF Collector. For more information, see “Installing and Configuring the Universal CEF Collector” on page 15.</td>
</tr>
<tr>
<td>4.7.x, where x is 2 and above</td>
<td>If CEF auditing is enabled.</td>
<td>None</td>
</tr>
<tr>
<td>4.8</td>
<td>Identity Manager is freshly installed.</td>
<td>None</td>
</tr>
</tbody>
</table>
2 Configuring NetIQ Sentinel with Identity Manager

Use the following checklist to verify that all of the steps are completed to install and configure Sentinel with Identity Manager.

☐ Install and configure Sentinel. NetIQ recommends that you install Identity Manager and Sentinel on different servers. For more information, see the NetIQ Sentinel Installation Guide.

☐ Install and configure the NetIQ Sentinel Universal CEF Collector. For more information, see Chapter 3, “Installing and Configuring the Sentinel Collectors,” on page 15.

☐ Install and configure the Syslog Connector. For more information, see Chapter 4, “Installing the Syslog Connector,” on page 17.

☐ Configure Identity Manager components to use Common Event Format (CEF).
   For more information, see Chapter 5, “Configuring Identity Manager Components to Log Audit Events in CEF Format,” on page 19.

☐ Configure the Sentinel Control Center to access the predefined reports for Identity Manager.
3 Installing and Configuring the Sentinel Collectors

You must install and configure the Sentinel collectors which will parse and normalize the raw data to
the respective connectors and then convert the data into a Sentinel event.

The collectors must be added to the Event Source Manager to be installed. This step is only done
once. The added collectors are then displayed during configuration.

NOTE: After fresh installation of Sentinel with the required collectors and connectors installed and
configured, restart Sentinel for the changes to take effect.

Installing and Configuring the Universal CEF Collector

The Universal CEF Collector parses non-event data and transform the raw scan data into a format
understood by Sentinel. Sentinel then stores the vulnerability data in the database and includes it in
the Exploit Detection map. For more detailed information about Sentinel collectors, see the Sentinel

To install the Universal CEF Collector,

1 Download the latest Universal CEF Collector (.zip file) from the Sentinel Plug-ins website
2 Log in to the Sentinel Control Center.
3 Select the Event Source Management > Live View, then select Tools > Import plugin.
4 Browse to and select the .zip file you just downloaded, then click Next.
5 Follow the remaining prompts, then click Finish.

The Universal CEF Collector must be configured to work. To configure the Universal CEF Collector,

1 In the Event Source Management live view, right-click Sentinel Server, then click Add Collector.
2 Select Universal in the Vendor column.
3 Select Common Event Format in the Name column, then click Next.
4 From the Installed Collectors column, select Universal_Common-Event-Format_Collector_Version,
   then click Next. For example, Universal Common Event Format 2011.1r4.
5 Follow the prompts and click Finish.

The next step is to proceed to Chapter 4, “Installing the Syslog Connector,” on page 17.
Installing and Configuring the SSPR Collectors

To install the SSPR Collector,

1. Download the latest SSPR Collector (.zip file) from the NetIQ Plug-ins website.
2. Log in to the Sentinel Control Center.
3. Select the Event Source Management > Live View, then select Tools > Import plugin.
4. Browse to and select the .zip file you just downloaded, then click Next.
5. Follow the remaining prompts, then click Finish.

The SSPR Collector must be configured to work. To configure the SSPR Collector,

1. In the Event Source Management live view, right-click Sentinel Server, then click Add Collector.
2. Select NetIQ in the Vendor column.
3. Select Identity Manager in the Name column, then click Next.
4. From the Installed Collectors column, select `<Collector>_<Collector_Version>`, then click Next.
   
   For example: SelfServicePasswordReset_<Collector_Version>
5. Follow the prompts and click Finish.

For SSPR, the next step is to proceed to “Installing and Configuring the Syslog Connector” on page 17.
Installing the Syslog Connector

The Syslog Connector facilitates integration between Identity Manager and Sentinel. You must install and configure the Universal CEF Collector before you install and configure the Syslog Connector.

**NOTE:** After installing Sentinel with the required collectors and connectors installed and configured, restart Sentinel for the changes to take effect.

Installing and Configuring the Syslog Connector

To set up the connection with the Event Source, you must install the Syslog Connector plug-in.

Perform the following actions to install the Syslog Connector plug-in:

1. Download the latest Syslog Connector (.zip file) from the Sentinel Plug-ins website (https://marketplace.microfocus.com/cyberres/category/sentinel). The Syslog Connector is located under the Connectors tab. Save the file to the local computer where you want to run Event Source Management.
2. Log in to the Sentinel Control Center.
3. Go to the Event Source Management menu, and select the Live View option. For more information, see Configuring Data Collection for Syslog Event Sources in the Sentinel Administration Guide.
4. Select Tools > Import plug-in to display the Plug-in Import Type window.
5. In the Plug-in Import Type window, select the Import Collector or Connector plug-in package file (.zip, .clz, .cnz) option.
6. Click Next.
7. In the Choose Plug-in Package File window, browse to and select the Connector file you just downloaded.
8. Follow the remaining Import Plug-In Wizard instructions to import the Connector into the plug-in repository.
   - If another version of this Connector is already in use, you can click View Deployed Plug-ins to see which Event Source objects use the deployed Connectors.
9. (Optional) To update the deployed Connectors, select Update Deployed Plug-ins.
10. Click Finish.
Installing the Syslog Connector
5 Configuring Identity Manager Components to Log Audit Events in CEF Format

Identity Manager introduces Common Event Format (CEF), an open log management standard for auditing events across all Identity Manager components. CEF enables you to use a common event log format so that auditing data can easily be collected and aggregated for further analysis. CEF uses the Syslog message format as a transport mechanism.

Advantages of CEF

Previous versions of Identity Manager used a combination of different auditing solutions. Identity Manager now supports CEF to provide a uniform auditing solution across all Identity Manager components that can help improve your experience of configuring and working with auditing.

CEF uses a standard Syslog message format that simplifies log management. This enables you to integrate disparate Identity Manager data in your enterprise. The new event format seamlessly integrates with Sentinel.

Setting up CEF Configuration

After you install Identity Manager, ensure that all Identity Manager components are configured to generate the CEF events. To configure the components, see the following sections:

- “Configuring Identity Manager Engine” on page 20
- “Configuring Remote Loader” on page 20
- “Configuring .NET Remote Loader” on page 21
- “Configuring Java Remote Loader” on page 21
- “Configuring Fanout Agent” on page 22
- “Configuring Identity Applications” on page 22
- “Configuring Identity Reporting” on page 25
- “Configuring Data Collection Services” on page 25
- “Configuring One SSO Provider” on page 26
- “Configuring Self Service Password Reset” on page 27

IMPORTANT: If Identity Manager loses communication with the Sentinel server, Java Remote Loader, Fanout agent, and DCS events are not logged in the cache file for an approximate duration of two minutes. After the connection is restored, any cached events are sent to Sentinel after a delay of two minutes. There is no loss of events when Sentinel is normally shut down.

The CEF configuration settings are stored in a simple, text-based files for each component. For more information, see Understanding the Properties Files for CEF Auditing.
Before configuring the Identity Manager components, ensure that the Universal CEF Collector is configured in the Sentinel server. To log events with Universal CEF collector, ensure that the collector version is latest. For information about installing and configuring the Universal CEF collector, see Installing and Configuring the Sentinel Collectors.

Configuring Identity Manager Engine

The Identity Manager engine provides events for auditing. The configuration settings for Identity Manager Engine is stored in the `auditlogconfig.properties.template` file.

Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where Identity Manager Engine is installed.
2. Navigate to the directory where the `auditlogconfig.properties.template` file is present. By default, the file is located in the following directory:
   - Linux: `/etc/opt/novell/eDirectory/conf/`
   - Windows: `<eDirectory_install_path>\eDirectory\Conf`
3. Rename the `auditlogconfig.properties.template` file as `auditlogconfig.properties`.
4. Edit the `auditlogconfig.properties` file. Uncomment and update the appenders by removing `#` before each property. For more information, see “Identity Manager Engine, Remote Loader, and .NET Remote Loader” on page 53 in Understanding the `auditlogconfig.properties` File section.
5. Restart the Identity Vault.

To select events for auditing in CEF, use iManager.

1. Log in to iManager.
2. Select `Identity Manager Administration > Identity Manager Overview`.
3. Browse to and select the driver set object that contains the driver.
4. Select the driver set objects that contains the driver.
5. Click `Driver Set` and then click `Edit Driver Set properties`.
6. Click the `Log Level` tab, select the `Log specific events` radio button, and then click `OK`.
7. Select the events you want to log and click `OK`.

For the list of Identity Manager engine events, see Engine Events.

Configuring Remote Loader

The configuration settings for Remote Loader is stored in the `auditlogconfig.properties.template` file.

**NOTE:** CEF logging in Remote Loader will be enabled only if the `auditlogconfig.properties` file exists.
Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where Remote Loader is installed.
2. Navigate to the directory where the `auditlogconfig.properties.template` file is present. By default, the file is located in the following directory:
   - Linux: /etc/opt/novell/eDirectory/conf/
   - Windows: `<remote_loader_installed_location>\<processor_type>`
3. Rename the `auditlogconfig.properties.template` file as `auditlogconfig.properties`.
4. Edit the `auditlogconfig.properties` file. Uncomment and update the appenders by removing `#` before each property. For more information, see “Identity Manager Engine, Remote Loader, and .NET Remote Loader” on page 53 in `Understanding the auditlogconfig.properties File` section.
5. Restart Tomcat service.

For the list of Remote Loader events, see Remote Loader Events.

**Configuring .NET Remote Loader**

The configuration settings for .NET Remote Loader is stored in the `auditlogconfig.properties.template` file.

**NOTE:** The .NET Remote Loader is applicable for Windows only.

Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where .NET Remote Loader is installed.
2. Navigate to the directory where the `auditlogconfig.properties.template` file is present. By default, the file is located at:
   products\IDM\windows\setup\remoteloader.NET
3. Rename the `auditlogconfig.properties.template` file as `auditlogconfig.properties`.
4. Edit the `auditlogconfig.properties` file. Uncomment and update the appenders by removing `#` before each property. For more information, see “Identity Manager Engine, Remote Loader, and .NET Remote Loader” on page 53 in `Understanding the auditlogconfig.properties File` section.
5. Restart Tomcat service.

**Configuring Java Remote Loader**

**NOTE:** Ensure that the Rolling File Appender directory is present in `/var/opt/novell/eDirectory/log/cef-events.log` location for Java Remote Loader. Otherwise, Rolling File Appender directory will not work and no events will be logged.

The configuration settings for Java Remote Loader is stored in the `auditlogconfig.properties.template` file.
Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where Java Remote Loader is installed.
2. Navigate to the directory where the `auditlogconfig.properties.template` file is present. By default, the file is located at:
   - Linux: `<extracted loc of dirxml_jremote.tar.gz>/doc`
   - Windows: `<extracted loc of dirxml_jremote.tar.gz>/doc`
3. Rename the `auditlogconfig.properties.template` file as `auditlogconfig.properties`.
4. Edit the `auditlogconfig.properties` file. Uncomment and update the appenders by removing `#` before each property. For more information, see “Java Remote Loader and Fanout Agent” on page 57 in *Understanding the auditlogconfig.properties File* section.
5. To run the Java Remote Loader, specify the following command:
   ```bash
dirxml_jremote -config <Remote Loader configuration file> -auditlogfile /<PATH of the directory where auditlogconfig.properties file is located>/auditlogconfig.properties
   ```
6. Restart Tomcat service.

For a list of Java Remote Loader events, see Remote Loader Events.

### Configuring Fanout Agent

**NOTE:** Ensure that the Rolling File Appender directory is present in `/var/opt/novell/eDirectory/log/cef-events.log` location for Fanout Agent. Otherwise, Rolling File Appender directory will not work and no events will be logged.

When you run the Fanout agent for the first time, the `auditlogconfig.properties.template` file is created and located in the following directories:

- **Linux:** `/opt/novell/dirxml/fanoutagent/config`
- **Windows:** `<install-location>\FanoutAgent\config`

For the list of events, see Fanout Agent Events.

### Configuring Identity Applications

To configure settings for enabling CEF auditing, perform the following steps:

1. Log in to the Identity Applications server.
2. Navigate to the directory where `idmuserapp_logging.xml` and `workflow_logging.xml` files are located.
   - Linux: `/opt/netiq/idm/apps/tomcat/conf`
   - Windows: `<apps_install_path>\idm\apps\tomcat\conf`
Configuring Identity Manager Components to Log Audit Events in CEF Format

NOTE: •The workflow_logging.xml file is applicable for Identity Manager 4.8 version only.
  • By default, Identity Manager saves the logging configuration in idmuserapp_logging.xml file. However, the workflow events are generated only if CEF auditing is enabled in workflow_logging.xml file.

3 Add the CEF appenders and loggers in idmuserapp_logging.xml and workflow_logging.xml files. For more information, see “Understanding the idmuserapp_logging.xml File” on page 58 and “Understanding the workflow_logging.xml File” on page 61. NetIQ recommends you to retain the default value for the parameters in the appenders and loggers section.

NOTE: If you have upgraded to Identity Manager 4.8, you must ensure that all XDAS configuration and Naudit appenders and loggers have been deleted from the idmuserapp_logging.xml file.

4 (Conditional) Specify an intermediate event store directory to store and back up the events. Make sure that the permission and ownership are changed to novlua for that directory. To change the permission of the directory, run the following commands:

```
chown novlua:novlua <directory_path>
chmod 755 <directory_path>
```

where <directory_path> is path to the intermediate event store directory.

IMPORTANT: If you do not provide the required permissions to the intermediate event store directory, then:
  • you may not be able to access Identity Applications.
  • the OSP events will not be logged to the intermediate event store directory.

For Windows platform, provide the Administrative permission to the directory.

5 You can enable CEF auditing through either Identity Manager Dashboard or using configuration update utility.

To enable CEF auditing through Identity Manager Dashboard:

1. Log in to Identity Manager Dashboard as an administrator.
2. Select Configuration > Logging.
3. Click Auditing Configuration drop-down menu and select Enable CEF format. Specify the following auditing server details to use CEF format:
To enable CEF auditing through configuration update utility:

1. Navigate to the `/opt/netiq/idm/apps/configupdate` directory.
2. Run the following command: `./configupdate.sh`
3. In the CEF Auditing tab, select `Send audit events` check box and specify the following auditing server details to use CEF format:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination host</td>
<td>Specifies the destination hostname or IP address of the auditing server.</td>
</tr>
<tr>
<td>Destination port</td>
<td>Specifies the destination port number of the auditing server.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Specifies the protocol that should be used to establish communication with the auditing server. To establish a secure communication with the auditing server, select TCP protocol and enable Use TLS option. Provide the Keystore file name and the Keystore password.</td>
</tr>
<tr>
<td>Intermediate event store directory</td>
<td>Specifies the temporary directory where the events can be stored. This directory serves as a backup for an auditing server. If Identity Applications is freshly installed, the directory path will be populated by default. You can also provide path to intermediate event store directory of your choice. For more information, see Step 4.</td>
</tr>
</tbody>
</table>

4. Click Apply.

**To enable CEF auditing through configuration update utility:**

1. Navigate to the `/opt/netiq/idm/apps/configupdate` directory.
2. Run the following command: `./configupdate.sh`
3. In the CEF Auditing tab, select `Send audit events` check box and specify the following auditing server details to use CEF format:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination host</td>
<td>Specifies the destination hostname or IP address of the auditing server.</td>
</tr>
<tr>
<td>Destination port</td>
<td>Specifies the destination port number of the auditing server.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Specifies the protocol that should be used to establish communication with the auditing server. To establish a secure communication with the auditing server, select TCP protocol and enable Use TLS option. Provide the Keystore file name and the Keystore password.</td>
</tr>
<tr>
<td>Intermediate event store directory</td>
<td>Specifies the temporary directory where the events can be stored. This directory serves as a backup for an auditing server. If Identity Applications is freshly installed, the directory path will be populated by default. You can also provide path to intermediate event store directory of your choice. For more information, see Step 4.</td>
</tr>
</tbody>
</table>

4. Click OK.

6. Restart Tomcat.

For the list of identity applications events, see [Identity Applications Events](#).
Configuring Identity Reporting

The configuration settings for Identity Reporting auditing is stored in the idmrptcore_logging.xml file.

**NOTE:** You must use Sentinel 8.2 (or later) and Universal CEF collector version 2011.1r4 (or later) to log the events.

Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where you have installed Identity Reporting.
2. Navigate to the directory where idmrptcore_logging.xml file is present. By default, the file is located in the following directories:
   - **Linux:** /opt/netiq/idm/apps/tomcat/conf
   - **Windows:** C:\netiq\idm\apps\tomcat\conf
3. Add the following in the idmrptcore_logging.xml file:
   ```xml
   <audit>
   <syslog>
       <enabled>true</enabled>
       <protocol>TCP</protocol>
       <host>IP Address of your auditing server</host>
       <port>Auditing server port</port>
       <cache-dir>name of the cache directory</cache-dir>
       <cache-file>name of the cache file within the cache directory</cache-file>
       <application>Reporting Core</application>
       <vendor>Micro Focus</vendor>
       <version>6.0</version>
   </syslog>
   </audit>
   ```
   You must specify the Identity Reporting version number in the `<version>` element. For example, 6.0.
   
   For sample idmrptcore_logging.xml file, see “Understanding the idmrptcore_logging.xml File” on page 64.
4. Restart Tomcat service.

For the list of Identity Reporting events, see Identity Reporting Events.

Configuring Data Collection Services

The configuration settings for DCS auditing is stored in the idmrptdcs_logging.xml file.

Perform the following steps to configure settings for enabling CEF auditing:

1. Log in to the server where Data Collection Services is running.
2. Navigate to the directory where idmrptdcs_logging.xml file is present. By default, the file is located in the following directories:
   - **Linux:** /opt/netiq/idm/apps/tomcat/conf
3 Edit the `idmrptdcs_logging.xml` file. Uncomment and update the appenders by removing # before each property. For more information, see “Understanding the idmrptdcs_logging.xml File” on page 62.

4 Restart Tomcat service.

**NOTE:** You can define the Rolling File Appender directory and the cache directory. Make sure that you set the `novlua` permission for these directory, otherwise, Rolling File Appender or the cache directory will not work and no events will be logged. For example, you can change the permission and ownership of the directory using the `chown novlua:novlua /<directorypath>` command, where `<directorypath>` is the Rolling File Appender path or cache file directory path.

For a list of DCS events, see [DCS Events](#).

### Configuring One SSO Provider

When you have OSP and Identity Applications on the same server, the CEF auditing configuration performed on Identity Applications will apply to OSP (One SSO Provider) also. If OSP is installed on standalone server, then the configuration settings for OSP must be performed through the configuration update utility. For information on enabling CEF for OSP on Linux and Windows, see the following sections:

**Linux**

Launch the `configupdate.sh` from the `/opt/netiq/idm/apps/configupdate/` directory of the Identity Applications and define the values for the following CEF auditing parameters for the single sign-on client:

- **Send audit events**
  - Specifies whether you want to use CEF for auditing events.

- **Destination host**
  - Specifies the DNS name or the IP address of the auditing server.

- **Destination port**
  - Specifies the port of the auditing server.

- **Network protocol**
  - Specifies the network protocol used by the auditing server to receive CEF events.

- **Use TLS**
  - *Applies only when you want to use TCP as your network protocol.*
  - Specifies if the auditing server is configured to use TLS with TCP. Select **Use TLS > Show Advanced Options**, and provide the Identity Manager Keystore file name and the Identity Manager Keystore password.
Intermediate event store directory

Specifies the location of the cache directory before the CEF events are sent to the auditing server. If you are providing an intermediate event store directory of your choice, you must first ensure that the permission and ownership are set to novlua for that directory. To change the permission of the directory, run the following commands:

```
chown novlua:novlua <directory_path>
chmod 755 <directory_path>
```

where `<directory_path>` is the path to the intermediate event store directory.

Windows

Launch the `configupdate.bat` from the installation subdirectory for the Identity Applications (C:\NetIQ\idm\apps\UserApplication) and define the values for the following CEF Auditing parameters for the single sign-on client:

Send audit events

Specifies whether you want to use CEF for auditing events in Identity Applications.

Destination host

Specifies the DNS name or the IP address of the auditing server.

Destination port

Specifies the port of the auditing server.

Network Protocol

Specifies the network protocol used by the auditing server to receive CEF events.

Use TLS

*Applies only when you want to use TCP as your network protocol.*

Specifies if the auditing server is configured to use TLS with TCP.

Intermediate event store directory

Specifies the location of the cache directory before the CEF events are sent to the auditing server.

**NOTE:** Ensure that the `novlua` permissions are set for the Intermediate event store directory. Otherwise, you cannot access the IDMDash and IDMProv applications. Also, none of the OSP events will be logged in the Intermediate event store directory. For example, you can change the permission and ownership of the directory using the `chown novlua:novlua <directory>path` command, where `<directory>path` is the Intermediate event store directory.

Configuring Self Service Password Reset

For information on enabling CEF audit for SSPR, see Auditing for Self Service Password Reset in Self Service Password Reset Administration Guide.
Configuring Identity Manager Components to Log Audit Events in CEF Format
Securing the Logging System

The Sentinel server and some of the Identity Manager components utilize embedded certificates generated by an internal Certificate Authority (CA). These SSL certificates ensure that communication between the Identity Manager instrumentation and the Sentinel server is secure.

Enabling SSL Connection for User Application

To create a SSL certificate, perform the following actions:

1. Download the public certificate in .der format from the Sentinel server.

   For example, if you are using Mozilla Firefox as your browser that already has a certificate, use the following procedure to download the certificate.

   1a. Launch the Sentinel Server in your browser.
   1b. Click Show site information > View Certificate.
   1c. Go to Details tab and export the certificate in .der format.

2. Add the certificate to the Java keystore.

   For example, use the following command:

   ```
   keytool -import -file PATH_OF_DERFile\PublicKeyCert.der -keystore KEYSOTOERPATH\NAME.keystore -storepass keystorepass
   ```

   The next step is to define which events to log. Proceed to “Managing Identity Manager Events” on page 31.

Enabling SSL Connection for Identity Manager Engine

Perform the following steps to enable SSL connectivity for the Identity Manager Engine:

1. Login to the server where you have installed Identity Manager Engine.
2. Go to /etc/opt/novell/eDirectoery/conf folder.
3. Get the Sentinel Log Manager certificate and upload to keystore using the following command:

   ```
   echo | openssl s_client -connect <sentinel ip>:1443 >slm.pem
   ```

4. Edit the auditlogconfig.properties file. You must uncomment and update the appenders in the auditconfig.properties file. You can uncomment by removing the # before each property. For more information, see “Understanding the auditlogconfig.properties File” on page 53.

5. Save the auditconfig.properties file and exit.

6. Select those events that you want to audit from the driver set properties in iManager. For more information, see “Selecting Events for the Driver Set” on page 32.
7 Restart Identity Vault using the following commands:

ndsmanage stopall
ndsmanage startall
Managing Identity Manager Events

The event information sent to NetIQ Sentinel is managed through product-specific instrumentations, or plug-ins. The Identity Manager Instrumentation allows you to configure which events are logged to your data store. You can select predefined log levels, or you can individually select the events you want to log. You can also add user-defined events to the Identity Manager schema.

The following sections review how to manage Identity Manager events:

- “Selecting Events to Log” on page 31
- “User-Defined Events” on page 34
- “eDirectory Objects that Store Identity Manager Event Data” on page 35

Selecting Events to Log

The Identity Manager Instrumentation allows you to select events to be logged for the User Application, driver set, or a specific driver.

**NOTE:** Drivers can inherit logging configuration from the driver set.

- Selecting Events for the User Application
- Selecting Events for the Driver Set
- Selecting Events for a Specific Driver
- Identity Manager Log Levels

Selecting Events for the User Application

The User Application enables you to change the log level settings of individual loggers.

1. Log in to Identity Manager dashboard as an administrator.
2. Click Configuration > Logging.
3. Click Logging Configuration drop-down menu.
4. Enter the package name in the search.
5. Click Log level drop-down list and select one of the following log levels.

   Alternatively, you can select Change the log levels for the listed packages toggle button to change the log levels for the listed packages in bulk.

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fatal</td>
<td>Writes Fatal level messages to the log.</td>
</tr>
<tr>
<td>Error</td>
<td>Writes Fatal and Error level messages to the log.</td>
</tr>
</tbody>
</table>
Managing Identity Manager Events

6 Select **Persist the logging changes** to save the changes for any subsequent application server restarts.

7 Click **Apply**.

The User Application logging configuration is saved in `/opt/netiq/idm/apps/tomcat/conf/idmuserapp_logging.xml`.

### Selecting Events for the Driver Set

1 In iManager, select **Identity Manager > Identity Manager Overview**.

2 Browse to and select the driver set object.

3 Click the driver set object in the list of driver sets, then click **Driver Set > Edit Driver Set properties**.

4 Click the **Log Level** tab, then select a log level for the driver set.

   For an explanation of each log level, see Table 7-1, “Identity Manager Log Levels,” on page 33.

5 Enable the **Turn off logging to Driver Set, Subscriber and Publisher logs** option to prevent logging audit events to eDirectory.

   Enabling this option improves the performance of the Identity Manager system.

6 Click **Apply** or **OK** to save your changes.

**NOTE:** Changes to configuration settings are logged by default.

### Selecting Events for a Specific Driver

1 In iManager, select **Identity Manager > Identity Manager Overview**.

2 Browse to and select the driver set object that contains the driver

3 Select the driver set from the list of driver sets.

4 Click the upper right corner of the driver icon, then select **Edit properties**.

5 Select the **Log Level** tab.

6 (Optional) By default, the Driver object is configured to inherit log settings from the Driver Set object. To select logged events for this driver only, deselect **Use log settings from the Driver Set**.

---

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn</td>
<td>Writes Fatal, Error, and Warn level messages to the log.</td>
</tr>
<tr>
<td>Info</td>
<td>Writes Fatal, Error, Warn, and Info level messages to the log.</td>
</tr>
<tr>
<td>Debug</td>
<td>Writes Fatal, Error, Warn, Info, and debugging information to the log.</td>
</tr>
<tr>
<td>Trace</td>
<td>Writes Fatal, Error, Warn Info, debugging, and tracing information to the log.</td>
</tr>
</tbody>
</table>
7 Enable the Turn off logging to Driver Set, Subscriber and Publisher logs option. Enabling this option improves the performance of the Identity Manager system.

8 Select a log level for the current driver. For an explanation of each log level, see Table 7-1, “Identity Manager Log Levels,” on page 33.

9 Click Apply or OK to save your changes.

NOTE: Changes to configuration settings are logged by default.

Identity Manager Log Levels

The following table provides an explanation of the Identity Manager Instrumentation log levels:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log errors</td>
<td>This is the default log level. The Identity Manager Instrumentation logs user-defined events and all events with an error status. You receive only events with a decimal ID of 196646 and an error message stored in the Text1 field.</td>
</tr>
<tr>
<td>Log errors and warnings</td>
<td>The Identity Manager Instrumentation logs user-defined events and all events with an error or warning status. You receive only events with a decimal ID of 196646 or 196647 and an error or warning message stored in the first text field.</td>
</tr>
<tr>
<td>Log specific events</td>
<td>This option allows you to select the Identity Manager events you want to log. Click [] to select the specific events you want to log. After you select the events you want to log, click OK. For a list of all available events, see Appendix A, “Identity Manager Events,” on page 41.</td>
</tr>
<tr>
<td>Only update the last log time</td>
<td>The Identity Manager Instrumentation logs only user-defined events. When an event occurs, the last log time is updated so you can view the time and date of the last error in the status log.</td>
</tr>
<tr>
<td>Logging off</td>
<td>The Identity Manager Instrumentation logs only user-defined events. \n</td>
</tr>
<tr>
<td>Maximum Number of Entries in the Log</td>
<td>This setting allows you to specify the maximum number of entries to log in the status logs.</td>
</tr>
</tbody>
</table>
User-Defined Events

Identity Manager enables you to configure your own events to log to NetIQ Sentinel. Events can be logged by using an action in the Policy Builder, or within a style sheet. Any information you have access to when defining policies can be logged.

User-defined events are logged any time logging is enabled and are never filtered by the Identity Manager engine. You must use the policy builder to generate user-defined events.

You can specify any CEF key names in the Identity Manager policies and the specified key names will be reflected in the custom CEF event. For more information about updating the Identity Manager policies, see the *NetIQ Identity Manager - Using Designer to Create Policies*.

If you want to modify the custom CEF events, you can modify the Universal CEF collector to service the events:

2. From the extracted folder, modify the following files:
   - NetIQ_IDM_taxonomy.map - To customize the taxonomy for the user defined events.
   - NetIQ_Identity.Manager.map - To add and map new CEF fields to Sentinel fields.
   - idm.js - To modify the Record.prototype.processCustomEvents(e) function.

For more information, follow the steps mentioned in Sentinel plug-ins (https://marketplace.microfocus.com/cyberres/content/universal-common-event-format) documentation.

You can download the Sentinel plug-ins from the Sentinel download page. For more information about upgrading an existing collector, see Upgrade Procedures (https://marketplace.microfocus.com/cyberres/content/universal-common-event-format).

Using Policy Builder to Generate Events

1. In the Policy Builder, define the condition that must be met to generate the event, then select the Generate Event action.
2. Specify an event ID.
   
   Event IDs between 1000 and 1999 are allotted for user-defined events. You must specify a value within this range for the event ID when defining your own events. However, the event IDs between 1200 to 1203 are reserved for account related entitlement events and must not be used.
   
   The IDM event ID is combination of 30 and the hexadecimal of event ID.
   
   For example, if the ID provided in generate event policy action was 1344, then the IDM event ID is, “30” “hexadecimal of (1344)” = “30” “540” = “30540”.
3. Select a log level.
   
   Log levels enable you to group events based on the type of event being logged. The following predefined log levels are available:
Managing Identity Manager Events

4 Click the icon next to the Enter Strings field to launch the Named String Builder.

In the Named String Builder, you can specify any key and value pair. The output will display these values as the CEF extension fields for the event.

For more information and examples of the Generate Event action, see “Generate Event” in the NetIQ Identity Manager - Using Designer to Create Policies guide.

## eDirectory Objects that Store Identity Manager Event Data

The Identity Manager events you want to log are stored in the DirXML-LogEvents attribute on the Driver Set object or Driver object. The attribute is a multi-value integer with each value identifying an event ID to be logged.

You do not need to modify these attributes directly, because these objects are automatically configured based on your selections in iManager.

Before logging an event, the engine checks the current event type against the content of the DirXML-LogEvents attribute to determine whether the event should be logged.

Drivers can inherit log settings from the driver set. The DirXML-DriverTraceLevel attribute of a Driver object has the highest precedence when determining log settings. If a Driver object does not contain a DirXML-DriverTraceLevel attribute, the engine uses the log settings from the parent driver set.

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-emergency</td>
<td>10</td>
<td>Events that cause the Identity Manager engine or driver to shut down.</td>
</tr>
<tr>
<td>log-alert</td>
<td>9</td>
<td>Events that require immediate attention.</td>
</tr>
<tr>
<td>log-critical</td>
<td>8</td>
<td>Events that can cause parts of the Identity Manager engine or driver to malfunction.</td>
</tr>
<tr>
<td>log-error</td>
<td>7</td>
<td>Events describing errors that can be handled by the Identity Manager engine or driver.</td>
</tr>
<tr>
<td>log-warning</td>
<td>4</td>
<td>Negative events not representing a problem.</td>
</tr>
<tr>
<td>log-notice</td>
<td>2</td>
<td>Positive or negative events an administrator can use to understand or improve use and operation.</td>
</tr>
<tr>
<td>log-info</td>
<td>1</td>
<td>Positive events of any importance.</td>
</tr>
<tr>
<td>log-debug</td>
<td>0</td>
<td>Events of relevance for support or for engineers to debug the Identity Manager engine or driver.</td>
</tr>
</tbody>
</table>
Using Status Logs

In addition to the functionality provided by Sentinel, Identity Manager logs a specified number of events on the driver set and the driver. These status logs provide a view of recent Identity Manager activity. After the log reaches the set size, the oldest half of the log is permanently removed to clear room for more recent events. Therefore, any events you want to track over time should be logged to Sentinel.

The following sections contain information on the Identity Manager logs:

- “Setting the Log Level and Maximum Log Size” on page 37
- “Viewing Status Logs” on page 39

Setting the Log Level and Maximum Log Size

Status logs can be configured to hold between 50 and 500 events. This setting can be configured for the driver set to be inherited by all drivers in the driver set, or configured for each driver in the driver set. The maximum log size operates independently of the events you have selected to log, so you can configure the events you want to log for the driver set, then specify a different log size for each driver in the set.

This section reviews how to set the maximum log size on the driver set or an individual driver:

- “Setting the Log Level and Log Size for the Driver Set” on page 37
- “Setting the Log Level and Log Size for the Driver” on page 38

Setting the Log Level and Log Size for the Driver Set

1. In iManager, select Identity Manager > Identity Manager Overview.
2. Browse to and select the driver set.
3. Click the driver set name to access the driver set overview page.
4. Select Driver Set > Edit Driver Set properties.
5 Select Log Level.

6 Enable the Turn off logging to Driver Set, Subscriber and Publisher logs option to prevent logging audit events to eDirectory.
   Enabling this option improves the performance of the Identity Manager system.

7 Specify the maximum log size in the Maximum number of entries in the log field:

   Maximum number of entries in the log (50 - 500):  50

8 After you have specified the maximum number, click OK.

**Setting the Log Level and Log Size for the Driver**

1 In iManager select Identity Manager > Identity Manager Overview.
2 Browse to and select the driver set.
3 Click the driver set to access the driver set overview page.
4 Click the upper right corner of the driver icon, then select Edit properties.

5 Select Log Level.

6 Deselect Use log settings from the driver set option, if it is selected.

7 Specify the maximum log size in the Maximum number of entries in the log field:

   Maximum number of entries in the log (50 - 500):  50

8 After you have specified the maximum number, click OK.
Viewing Status Logs

The status logs are short-term logs for the driver set, the Publisher channel, and the Subscriber channel. They are accessed through different locations in iManager.

- “Accessing the Driver Set Status Log” on page 39
- “Accessing the Publisher Channel and Subscriber Channel Status Logs” on page 40

Accessing the Driver Set Status Log

The status log for the driver set contains only messages generated by the engine, such as state changes for any drivers in the driver set. All engine messages are logged. There are two ways to access the driver set status log:

- “Viewing the Log from the Driver Set Overview Page” on page 39
- “Viewing the Log from the Driver Overview Page” on page 39

Viewing the Log from the Driver Set Overview Page

1. In iManager, select Identity Manager > Identity Manager Overview.
2. Browse to and select the driver set.
3. Click the driver set to access the driver set overview page.
4. Select Driver Set > View status log.

Viewing the Log from the Driver Overview Page

1. In iManager, select Identity Manager > Identity Manager Overview.
2. Browse to and select the driver set.
3. Click the driver set to access the driver set overview page, then click any driver.
   The status log for the driver is stored on the driver overview page for each driver.
Click the Driver Set Status Log icon above the driver object.

1 In iManager, select Identity Manager > Identity Manager Overview.
2 Browse to and select the driver set.
3 Click the driver set to access the driver set overview page.
4 Click the desired driver object.
5 Click the Publisher channel or the Subscriber channel status log icon.

The status logs for the Publisher and Subscriber channels report channel-specific messages generated by the driver, such as an operation veto for an unassociated object.

To access the Publisher channel and the Subscriber channel logs:

1 In iManager, select Identity Manager > Identity Manager Overview.
2 Browse to and select the driver set.
3 Click the driver set to access the driver set overview page.
4 Click the desired driver object.
5 Click the Publisher channel or the Subscriber channel status log icon.
Identity Manager Events

This section provides a listing of all events logged by Identity Manager.

- “Event Structure” on page 41
- “Remote Loader Events” on page 41
- “Engine Events” on page 42
- “Fanout Agent Events” on page 45
- “Identity Applications Events” on page 45
- “Identity Reporting Events” on page 50
- “DCS Events” on page 50

Event Structure

All events logged through Sentinel have a standardized set of fields. This allows Sentinel to log events to a structured database and query events across all logging applications.

Identity Manager events provide information in the following field structure:

CEF:Version|Device Vendor|Device Product|Device Version|Event Number|Event Name|Severity|Extension

Remote Loader Events

The following table lists the Remote Loader events that can be audited through Sentinel:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>0030BB8</td>
<td>Remote Loader Start</td>
<td>Occurs when the Remote Loader starts.</td>
</tr>
<tr>
<td>0030BB9</td>
<td>Remote Loader Stop</td>
<td>Occurs when the Remote Loader stops.</td>
</tr>
<tr>
<td>0030BBA</td>
<td>Remote Loader Connection Established</td>
<td>Occurs when the engine establishes a TCP connection with the Remote Loader.</td>
</tr>
<tr>
<td>0030BBB</td>
<td>Remote Loader Connection Dropped</td>
<td>Occurs when the engine-to-Remote Loader connection is lost.</td>
</tr>
<tr>
<td>0030026</td>
<td>Invalid Response to challenge during command authentication</td>
<td>Occurs when you specify an incorrect password.</td>
</tr>
</tbody>
</table>
## Engine Events

The following table lists the engine events that can be audited through Sentinel:

### Table A-2  Engine Events

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>0030001</td>
<td>Status Success</td>
<td>Many different events can cause the status success event to occur. It usually signifies that an operation was successfully completed.</td>
</tr>
<tr>
<td>0030002</td>
<td>Status Retry</td>
<td>Many different events can cause the status retry event to occur. It signifies an operation was not completed and the operation must be tried again later.</td>
</tr>
<tr>
<td>0030003</td>
<td>Status Warning</td>
<td>Many different events can cause the status warning event to occur. It usually signifies that an operation was completed with minor problems.</td>
</tr>
<tr>
<td>0030004</td>
<td>Status Error</td>
<td>Many different events can cause the status error event to occur. It usually signifies that an operation was not completed successfully.</td>
</tr>
<tr>
<td>0030005</td>
<td>Status Fatal</td>
<td>Many different events can cause the status fatal event to occur. It usually signifies that an operation was not completed successfully and the engine or driver could not continue.</td>
</tr>
<tr>
<td>0030006</td>
<td>Status Other</td>
<td>Any status document processed with a level other than the five previously defined creates a status other event. These events can only be generated within a style sheet or rule.</td>
</tr>
<tr>
<td>0030007</td>
<td>Search</td>
<td>Occurs when a query document is sent to the Identity Manager engine or driver.</td>
</tr>
<tr>
<td>0030008</td>
<td>Add Entry</td>
<td>Occurs when an object is added.</td>
</tr>
<tr>
<td>0030009</td>
<td>Delete Entry</td>
<td>Occurs when an object is deleted.</td>
</tr>
<tr>
<td>003000A</td>
<td>Modify Entry</td>
<td>Occurs when an object is modified.</td>
</tr>
<tr>
<td>003000B</td>
<td>Rename Entry</td>
<td>Occurs when an object is renamed.</td>
</tr>
<tr>
<td>003000C</td>
<td>Move Entry</td>
<td>Occurs when an object is moved.</td>
</tr>
<tr>
<td>003000D</td>
<td>Add Association</td>
<td>Occurs when an association is added. It can happen on an add or a match.</td>
</tr>
<tr>
<td>003000E</td>
<td>Remove Association</td>
<td>When an object is deleted, there is no remove association event. The remove association occurs when a User object is deleted in the disparate application, and the delete is then converted into a modify that removes the association.</td>
</tr>
<tr>
<td>003000F</td>
<td>Query Schema</td>
<td>Occurs when a query schema operation is sent to the Identity Manager engine or driver.</td>
</tr>
<tr>
<td>0030010</td>
<td>Check User Password Status</td>
<td>Manual function that is initiated via iManager to check the status of the user’s password.</td>
</tr>
<tr>
<td>0030011</td>
<td>Check Object Password</td>
<td>Occurs when a request is issued to check an object's password, other than the driver.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Trigger</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 00307D7  | Keyed Password Set           | Occurs when a named password is modified. The following sub-event types for Keyed Password Set can be found under the act field of the CEF event:  
<p>|          |                              | - SET_NAMED_PASSWORD                                                   |
|          |                              | - CLEAR_NAMED_PASSWORD                                                 |
|          |                              | - CLEAR_ALL_NAMED_PASSWORD                                             |
|          |                              | - READ_ALL_NAMED_PASSWORD_KEYS                                         |
|          |                              | - SET_NAMED_PASSWORD                                                   |
|          |                              | - READ_ALL_NAMED_PASSWORD_KEYS_WITH_DISPLAY_STRINGS                    |
|          |                              | - SET_UTF8_NAMED_PASSWORD                                              |
| 0030012  | Change Password              | Occurs when a request is issued to change the driver's password.       |
| 0030013  | Sync                         | Occurs when a sync event is requested.                                 |
| 0030014  | Input XML Document           | Generated whenever an input document is created by the engine or driver.|
| 0030015  | Input Transformation Document| Generated after the input transformation policies are processed, allowing the user to view the transformed document. |
| 0030016  | Output Transformation Document| Generated after the output transformation policies are processed, allowing the user to view the transformed document. |
| 0030017  | Event Transformation Document| Generated after the event transformation policies are processed, allowing the user to view the transformed document. |
| 0030018  | Placement Rule Transformation Document| Generated after the Placement rule policies are processed, allowing the user to view the transformed document. |
| 0030019  | Create Rule Transformation Document| Generated after the Create rule policies are processed, allowing the user to view the transformed document. |
| 003001A  | Input Mapping Rule Transformation Document| Generated after the Schema Mapping rules are processed which convert the document to the eDirectory schema. |
| 003001B  | Output Mapping Rule Transformation Document| Generated after the Schema Mapping rules are processed which convert the document to the applications schema. |
| 003001C  | Matching Rule Transformation Document| Generated after the Matching rule policies are processed, allowing the user to view the transformed document. |</p>
<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>003001D</td>
<td>Command Transformation Document</td>
<td>Generated after the command transformation policies are processed, allowing the user to view the transformed document.</td>
</tr>
<tr>
<td>003001E</td>
<td>Publisher Filter Transformation Document</td>
<td>Generated after processing the notify filter on the Publisher channel, allowing the user to view the transformed document.</td>
</tr>
<tr>
<td>003001F</td>
<td>User Agent Request</td>
<td>Occurs when a User Agent XDS command document is sent to the Driver on the Subscriber channel.</td>
</tr>
<tr>
<td>0030020</td>
<td>Resync Driver</td>
<td>Occurs when a resync request is issued.</td>
</tr>
<tr>
<td>0030021</td>
<td>Migrate</td>
<td>Occurs when a migrate request is issued.</td>
</tr>
<tr>
<td>0030022</td>
<td>Driver Start</td>
<td>Occurs when a driver is started.</td>
</tr>
<tr>
<td></td>
<td>NOTE:</td>
<td>The CEF event displayed on the auditing server such as Sentinel does not fetch the Hostname/IP address details of iManager or Designer from where the driver was started.</td>
</tr>
<tr>
<td>0030023</td>
<td>Driver Stop</td>
<td>Occurs when a driver is stopped.</td>
</tr>
<tr>
<td></td>
<td>NOTE:</td>
<td>The CEF event displayed on the auditing server such as Sentinel does not fetch the Hostname/IP address details of iManager or Designer from where the driver was stopped.</td>
</tr>
<tr>
<td>0030024</td>
<td>Password Sync</td>
<td>Generated when setting the distribution or simple password on an object.</td>
</tr>
<tr>
<td>0030025</td>
<td>Password Reset</td>
<td>Generated when resetting the connected application password after a failed password sync operation.</td>
</tr>
<tr>
<td>0030026</td>
<td>DirXML Error</td>
<td>Generated whenever the engine throws an internal error.</td>
</tr>
<tr>
<td>0030027</td>
<td>DirXML Warning</td>
<td>Generated whenever the engine throws an internal warning.</td>
</tr>
<tr>
<td>0030028</td>
<td>Custom Operation</td>
<td>Occurs when an unknown operation appears in an input document. An example of known operations would be an add, delete, or modify.</td>
</tr>
<tr>
<td>0030029</td>
<td>Clear Attribute</td>
<td>Occurs when a modify operation contains a remove-all-value element.</td>
</tr>
<tr>
<td>003002A</td>
<td>Add Value - Modify Entry</td>
<td>Occurs when a value is added during the modification of an object.</td>
</tr>
<tr>
<td>003002B</td>
<td>Remove Value</td>
<td>Occurs when a modify operation contains a remove-value element.</td>
</tr>
<tr>
<td>003002C</td>
<td>Merge Entries</td>
<td>Occurs when two objects are being merged.</td>
</tr>
<tr>
<td>003002D</td>
<td>Get Named Password</td>
<td>Generated on a Get Named Password operation.</td>
</tr>
<tr>
<td>003002E</td>
<td>Reset Attributes</td>
<td>Occurs when a Reset document is issued on the publisher or Subscriber channels.</td>
</tr>
<tr>
<td>003002F</td>
<td>Add Value - Add Entry</td>
<td>Occurs when a value is added during the creation of an object.</td>
</tr>
<tr>
<td>0030030</td>
<td>Set SSO Credential</td>
<td>Occurs when a driver policy executes the do-set-sso-credential action.</td>
</tr>
</tbody>
</table>
The following table lists the Fanout Agent events that can be audited through Sentinel:

**Table A-3 Fanout Agent Events**

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>0030FA0</td>
<td>Fanout Agent Start</td>
<td>Occurs when the Fanout Agent starts.</td>
</tr>
<tr>
<td>0030FA1</td>
<td>Fanout Agent Stop</td>
<td>Occurs when the Fanout Agent stops.</td>
</tr>
<tr>
<td>0030FA2</td>
<td>Service Start, Instance Service</td>
<td>Occurs when the driver is started</td>
</tr>
<tr>
<td>0030FA3</td>
<td>Service Stop, Instance Service</td>
<td>Occurs when the driver is stopped.</td>
</tr>
</tbody>
</table>

**Fanout Agent Events**

The following table lists the Fanout Agent events that can be audited through Sentinel:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>0030031</td>
<td>Clear SSO Credential</td>
<td>Occurs when a driver policy executes the do-clear-sso-credential action.</td>
</tr>
<tr>
<td>0030032</td>
<td>Set SSO Passphrase</td>
<td>Occurs when a driver policy executes the do-clear-sso-credential action.</td>
</tr>
<tr>
<td>0030033</td>
<td>Startup Rule</td>
<td>Generated after the Startup policies are processed. Allows the user to view the transformed document.</td>
</tr>
<tr>
<td>0030034</td>
<td>Shutdown Rule</td>
<td>Generated after the Shutdown policies are processed. Allows the user to view the transformed document.</td>
</tr>
<tr>
<td>0030035</td>
<td>Send Mail</td>
<td>Occurs when a policy or job is executed where the send mail option is configured. This will trigger a job to send an e-mail.</td>
</tr>
<tr>
<td>0030036</td>
<td>Entitlement Operation</td>
<td>Occurs when the value of the DirXML-EntitlementResult changes.</td>
</tr>
<tr>
<td>000304B0</td>
<td>Account Create By Entitlement Grant</td>
<td>Occurs when an account is created by granting of an entitlement.</td>
</tr>
<tr>
<td>000304B1</td>
<td>Account Delete By Entitlement Revoke</td>
<td>Occurs when an account is deleted on revoking of the entitlement.</td>
</tr>
<tr>
<td>000304B2</td>
<td>Account Disable By Entitlement Revoke</td>
<td>Occurs when an account is disabled on revoking of the entitlement.</td>
</tr>
<tr>
<td>000304B3</td>
<td>Account Enable By Entitlement Grant</td>
<td>Occurs when an account is enabled by granting of an entitlement.</td>
</tr>
</tbody>
</table>

**Identity Applications Events**

The following table lists the User Application events that can be audited through Sentinel:
<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>31400</td>
<td>Delete Entity</td>
<td>Occurs when an entity is deleted</td>
</tr>
<tr>
<td>31401</td>
<td>Update Entity</td>
<td>Occurs when an entity is updated</td>
</tr>
<tr>
<td>31440</td>
<td>Create Entity</td>
<td>Occurs when an entity is created</td>
</tr>
<tr>
<td>31450</td>
<td>Create Proxy Definition Success</td>
<td>Occurs when the creation of an entity definition succeeds</td>
</tr>
<tr>
<td>31451</td>
<td>Create Proxy Definition Failure</td>
<td>Occurs when the creation of an proxy definition fails</td>
</tr>
<tr>
<td>31452</td>
<td>Update Proxy Definition Success</td>
<td>Occurs when an update to the proxy definition fails</td>
</tr>
<tr>
<td>31453</td>
<td>Update Proxy Definition Failure</td>
<td>Occurs when an update to the proxy definition fails</td>
</tr>
<tr>
<td>31454</td>
<td>Delete Proxy Definition Success</td>
<td>Occurs when the proxy definition is deleted successfully</td>
</tr>
<tr>
<td>31455</td>
<td>Delete Proxy Definition Failure</td>
<td>Occurs when the proxy definition is not deleted successfully</td>
</tr>
<tr>
<td>31456</td>
<td>Create Delegatee Definition Success</td>
<td>Occurs when the creation of a delegatee definition succeeds</td>
</tr>
<tr>
<td>31457</td>
<td>Create Delegatee Definition Failure</td>
<td>Occurs when the creation of a delegatee definition fails</td>
</tr>
<tr>
<td>31458</td>
<td>Update Delegatee Definition Success</td>
<td>Occurs when an update to the delegatee definition succeeds</td>
</tr>
<tr>
<td>31459</td>
<td>Update Delegatee Definition Failure</td>
<td>Occurs when an update to the delegatee definition fails</td>
</tr>
<tr>
<td>003145A</td>
<td>Delete Delegatee Definition Success</td>
<td>Occurs when the delegatee definition is deleted successfully</td>
</tr>
<tr>
<td>003145B</td>
<td>Delete Delegatee Definition Failure</td>
<td>Occurs when the deletion of a delegatee definition fails</td>
</tr>
<tr>
<td>003145C</td>
<td>Create Availability Success</td>
<td>Occurs when the creation of an availability succeeds</td>
</tr>
<tr>
<td>003145D</td>
<td>Create Availability Failure</td>
<td>Occurs when the creation of an availability fails</td>
</tr>
<tr>
<td>003145E</td>
<td>Delete Availability Success</td>
<td>Occurs when the deletion of an availability succeeds</td>
</tr>
<tr>
<td>003145F</td>
<td>Delete Availability Failure</td>
<td>Occurs when the deletion of an availability fails</td>
</tr>
<tr>
<td>31520</td>
<td>Workflow Error</td>
<td>Occurs when there is a workflow error</td>
</tr>
<tr>
<td>31521</td>
<td>Workflow Started</td>
<td>Occurs when the workflow starts</td>
</tr>
<tr>
<td>31522</td>
<td>Workflow Forwarded</td>
<td>Occurs when the workflow is forwarded</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Trigger</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>31523</td>
<td>Workflow Reassigned</td>
<td>Occurs when the workflow is reassigned</td>
</tr>
<tr>
<td>31524</td>
<td>Workflow Approved</td>
<td>Occurs when the workflow is approved</td>
</tr>
<tr>
<td>31525</td>
<td>Workflow Refused</td>
<td>Occurs when the workflow is refused</td>
</tr>
<tr>
<td>31526</td>
<td>Workflow Ended</td>
<td>Occurs when the workflow ends</td>
</tr>
<tr>
<td>31527</td>
<td>Workflow Claimed</td>
<td>Occurs when the workflow is claimed</td>
</tr>
<tr>
<td>31528</td>
<td>Workflow Unclaimed</td>
<td>Occurs when the workflow is not claimed</td>
</tr>
<tr>
<td>31529</td>
<td>Workflow Denied</td>
<td>Occurs when the workflow is denied</td>
</tr>
<tr>
<td>30312A</td>
<td>Workflow Completed</td>
<td>Occurs when the workflow is completed</td>
</tr>
<tr>
<td>30312B</td>
<td>Workflow Timedout</td>
<td>Occurs when the workflow timed out</td>
</tr>
<tr>
<td>30312C</td>
<td>User Message</td>
<td>This is a user adhoc log message</td>
</tr>
<tr>
<td>3152D</td>
<td>Provision Error</td>
<td>Occurs when there is an error in the provisioning step</td>
</tr>
<tr>
<td>3152E</td>
<td>Provision Submitted</td>
<td>Occurs during the provisioning step on submission of entitlements.</td>
</tr>
<tr>
<td>30312F</td>
<td>Provision Success</td>
<td>Occurs during the provisioning step on successful completion of the step</td>
</tr>
<tr>
<td>31530</td>
<td>Provision Failure</td>
<td>Occurs during the provisioning step upon failure of the step</td>
</tr>
<tr>
<td>31531</td>
<td>Provision Granted</td>
<td>Occurs during the provisioning step on granting of an entitlement</td>
</tr>
<tr>
<td>31532</td>
<td>Provision Revoked</td>
<td>Occurs during the provisioning step on the revoking of an entitlement</td>
</tr>
<tr>
<td>31533</td>
<td>Workflow Retracted</td>
<td>Occurs when the workflow is retracted</td>
</tr>
<tr>
<td>31534</td>
<td>Workflow Escalated</td>
<td>Occurs when the workflow is escalated</td>
</tr>
<tr>
<td>31535</td>
<td>Workflow Reminder Sent</td>
<td>Occurs when reminders are sent to addressees of a workflow task</td>
</tr>
<tr>
<td>31536</td>
<td>Digital Signature</td>
<td>Occurs whenever a digital signature is passed to the workflow engine</td>
</tr>
<tr>
<td>31537</td>
<td>Workflow ResetPriority</td>
<td>Occurs when the priority of a workflow task is reset.</td>
</tr>
<tr>
<td>31538</td>
<td>Role Approved</td>
<td>Occurs when a role is approved</td>
</tr>
<tr>
<td>31539</td>
<td>Role Denied</td>
<td>Occurs when a role is denied</td>
</tr>
<tr>
<td>30313A</td>
<td>SOD Exception Approved</td>
<td>Occurs when an SOD exception is approved</td>
</tr>
<tr>
<td>30313B</td>
<td>SOD Exception Denied</td>
<td>Occurs when an SOD exception is denied</td>
</tr>
<tr>
<td>30313C</td>
<td>Start Correlated Workflow</td>
<td>Occurs when a correlated workflow is started</td>
</tr>
<tr>
<td>30313D</td>
<td>Role Request Submitted</td>
<td>Occurs when a role request is submitted</td>
</tr>
<tr>
<td>3153E</td>
<td>Resource Approved</td>
<td>Occurs when a resource is approved</td>
</tr>
<tr>
<td>30313F</td>
<td>Resource Denied</td>
<td>Occurs when a resource is denied</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Trigger</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>31540</td>
<td>Provision Already Exists</td>
<td>Occurs when a request for PRD with workflow contains provisioning</td>
</tr>
<tr>
<td>31541</td>
<td>Resource Request Submitted</td>
<td>Occurs when a request for a resource is submitted</td>
</tr>
<tr>
<td>31542</td>
<td>Resource Provisioning Workflow Submitted</td>
<td>Occurs when a resource provisioning workflow is submitted</td>
</tr>
<tr>
<td>31543</td>
<td>Resource Provisioning Workflow Failed</td>
<td>Occurs when a resource provisioning workflow fails</td>
</tr>
<tr>
<td>31544</td>
<td>Workflow Returned</td>
<td>Occurs when the role is returned to user task</td>
</tr>
<tr>
<td>31550</td>
<td>Login Success</td>
<td>Occurs when the login succeeds</td>
</tr>
<tr>
<td>31551</td>
<td>Login Failure</td>
<td>Occurs when the login fails</td>
</tr>
<tr>
<td>31600</td>
<td>Role Provisioning</td>
<td>Occurs when a role is provisioned</td>
</tr>
<tr>
<td>31601</td>
<td>Role Provisioning Failure</td>
<td>Occurs when a role provisioning fails</td>
</tr>
<tr>
<td>31610</td>
<td>Role Request</td>
<td>Occurs when a role is requested</td>
</tr>
<tr>
<td>31611</td>
<td>Role Request Failure</td>
<td>Occurs when the request for a role fails</td>
</tr>
<tr>
<td>31612</td>
<td>Role Request Workflow</td>
<td>Occurs when a role with an approver is requested</td>
</tr>
<tr>
<td>31613</td>
<td>SOD Exception Auto Approval</td>
<td>Occurs when the SOD exception is auto approved</td>
</tr>
<tr>
<td>31614</td>
<td>Retract Role Request</td>
<td>Occurs when the role request is retracted</td>
</tr>
<tr>
<td>31615</td>
<td>Retract Role Request Failure</td>
<td>Occurs when the retraction of a role request fails</td>
</tr>
<tr>
<td>31620</td>
<td>Entitlement Grant</td>
<td>Occurs when the entitlement is granted</td>
</tr>
<tr>
<td>31621</td>
<td>Entitlement Grant Failure</td>
<td>Occurs when the entitlement grant fails</td>
</tr>
<tr>
<td>31622</td>
<td>Entitlement Revoke</td>
<td>Occurs when the entitlement is revoked</td>
</tr>
<tr>
<td>31623</td>
<td>Entitlement Revoke Failure</td>
<td>Occurs when the entitlement revoke fails</td>
</tr>
<tr>
<td>31624</td>
<td>Entitlement Invalid Reference</td>
<td>Occurs when the DirXML-EntitlementRef xml is not valid</td>
</tr>
<tr>
<td>31630</td>
<td>Create Role</td>
<td>Occurs when a role is created</td>
</tr>
<tr>
<td>31631</td>
<td>Create Role Failure</td>
<td>Occurs when creating a role fails</td>
</tr>
<tr>
<td>31632</td>
<td>Delete Role</td>
<td>Occurs when a role is deleted</td>
</tr>
<tr>
<td>31634</td>
<td>Modify Role</td>
<td>Occurs when a role is modified</td>
</tr>
<tr>
<td>31635</td>
<td>Modify Role Failure</td>
<td>Occurs when modifying a role fails</td>
</tr>
<tr>
<td>31640</td>
<td>Create SOD</td>
<td>Occurs when SOD is created</td>
</tr>
<tr>
<td>31641</td>
<td>Create SOD Failure</td>
<td>Occurs when creating SOD fails</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Trigger</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>31642</td>
<td>Delete SOD</td>
<td>Occurs when SOD is deleted</td>
</tr>
<tr>
<td>31644</td>
<td>Modify SOD</td>
<td>Occurs when SOD is modified</td>
</tr>
<tr>
<td>31645</td>
<td>Modify SOD Failure</td>
<td>Occurs when modifying SOD fails</td>
</tr>
<tr>
<td>31660</td>
<td>Resource Request</td>
<td>Occurs when a resource is requested</td>
</tr>
<tr>
<td>31662</td>
<td>Resource Request Workflow</td>
<td>Occurs when a resource is requested as a normal user</td>
</tr>
<tr>
<td>31663</td>
<td>Retract Resource Request</td>
<td>Occurs when a resource request is retracted</td>
</tr>
<tr>
<td>31665</td>
<td>Resource Provisioning</td>
<td>Occurs when a resource is provisioned</td>
</tr>
<tr>
<td>31666</td>
<td>Resource Provisioning Failure</td>
<td>Occurs when resource provisioning fails</td>
</tr>
<tr>
<td>31667</td>
<td>Resource Provisioning Workflow</td>
<td>Occurs when a resource provisioning workflow is requested</td>
</tr>
<tr>
<td>31670</td>
<td>Create Resource</td>
<td>Occurs when a resource is created</td>
</tr>
<tr>
<td>31671</td>
<td>Create Resource Failure</td>
<td>Occurs when resource creation fails</td>
</tr>
<tr>
<td>31672</td>
<td>Delete Resource</td>
<td>Occurs when a resource is deleted</td>
</tr>
<tr>
<td>31674</td>
<td>Modify Resource</td>
<td>Occurs when a resource is modified</td>
</tr>
<tr>
<td>31675</td>
<td>Modify Resource Failure</td>
<td>Occurs when modifying a resource fails</td>
</tr>
<tr>
<td>31676</td>
<td>Create Resource Association</td>
<td>Occurs when creating resource association</td>
</tr>
<tr>
<td>31677</td>
<td>Create Resource Association Failure</td>
<td>Occurs when creating resource association fails</td>
</tr>
<tr>
<td>31678</td>
<td>Delete Resource Association</td>
<td>Occurs when deleting a resource association</td>
</tr>
<tr>
<td>31680</td>
<td>Create Domain Administrator</td>
<td>Occurs when creating a domain administrator</td>
</tr>
<tr>
<td>31681</td>
<td>Create Domain Administrator Failure</td>
<td>Occurs when creating a domain administrator fails</td>
</tr>
<tr>
<td>31682</td>
<td>Delete Domain Administrator</td>
<td>Occurs when deleting a domain administrator</td>
</tr>
<tr>
<td>31683</td>
<td>Delete Domain Administrator Failure</td>
<td>Occurs when deleting a domain administrator fails</td>
</tr>
<tr>
<td>31684</td>
<td>Create Delegated Administrator</td>
<td>Occurs when creating a delegated administrator</td>
</tr>
<tr>
<td>31685</td>
<td>Create Delegated Administrator Failure</td>
<td>Occurs when creating a delegated administrator fails</td>
</tr>
<tr>
<td>31686</td>
<td>Delete Delegated Administrator</td>
<td>Occurs when deleting a delegated administrator</td>
</tr>
</tbody>
</table>
Identity Reporting Events

The following table lists Identity Reporting events that can be audited through Sentinel:

*Table A-5  Identity Reporting Events*

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>31687</td>
<td>Delete Delegated Administrator Failure</td>
<td>Occurs when deleting a delegated administrator fails</td>
</tr>
<tr>
<td>31688</td>
<td>Create Team</td>
<td>Occurs when creating a team</td>
</tr>
<tr>
<td>31689</td>
<td>Create Team Failure</td>
<td>Occurs when creating a team fails</td>
</tr>
<tr>
<td>31690</td>
<td>Delete Team</td>
<td>Occurs when deleting a team</td>
</tr>
<tr>
<td>31691</td>
<td>Delete Team Failure</td>
<td>Occurs when deleting a team fails</td>
</tr>
<tr>
<td>31692</td>
<td>Modify Team</td>
<td>Occurs when a team is modified</td>
</tr>
<tr>
<td>31693</td>
<td>Modify Team Failure</td>
<td>Occurs when modifying a team fails</td>
</tr>
<tr>
<td>31694</td>
<td>Create Authorization</td>
<td>Occurs when the permissions are assigned to the team</td>
</tr>
<tr>
<td>31695</td>
<td>Delete Authorization</td>
<td>Occurs when the permissions are removed from the team</td>
</tr>
</tbody>
</table>

DCS Events

The following table lists Data Collection Service events that can be audited through Sentinel:

*Table A-6  DCS Events*

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>00031721</td>
<td>DCS Driver Registration Add</td>
<td>Occurs when the DCS driver is added</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Trigger</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>00031722</td>
<td>DCS Driver Registration Modify</td>
<td>Occurs when the DCS driver is modified</td>
</tr>
<tr>
<td>00031723</td>
<td>DCS Driver Collection enabled</td>
<td>Occurs when the data collection is enabled</td>
</tr>
<tr>
<td>00031724</td>
<td>DCS Driver Collection disabled</td>
<td>Occurs when the data collection is disabled</td>
</tr>
<tr>
<td>00031728</td>
<td>Data Collection Suspended</td>
<td>Occurs when the data collection is suspended</td>
</tr>
<tr>
<td>00031729</td>
<td>Data Collection Activated</td>
<td>Occurs when the data collection is activated</td>
</tr>
<tr>
<td>00031730</td>
<td>Data Collection Started</td>
<td>Occurs when the data collection is started</td>
</tr>
<tr>
<td>00031731</td>
<td>Data Collection Completed</td>
<td>Occurs when the data collection is completed</td>
</tr>
<tr>
<td>00031732</td>
<td>Data Collection Failed</td>
<td>Occurs when the data collection fails</td>
</tr>
<tr>
<td>00031733</td>
<td>Data Collection Requested</td>
<td>Occurs when the data collection is requested</td>
</tr>
<tr>
<td>00031734</td>
<td>Data Cleanup Requested</td>
<td>Occurs when the data cleanup is requested</td>
</tr>
<tr>
<td>00031735</td>
<td>Data Cleanup Started</td>
<td>Occurs when the data cleanup is started</td>
</tr>
<tr>
<td>00031736</td>
<td>Data Cleanup Completed</td>
<td>Occurs when the data cleanup is completed</td>
</tr>
<tr>
<td>00031736</td>
<td>Data Cleanup Failed</td>
<td>Occurs when the data cleanup fails</td>
</tr>
</tbody>
</table>
Understanding the Properties Files for CEF Auditing

The appendix provides details about the properties files used by the different components of Identity Manager for auditing through CEF.

Understanding the auditlogconfig.properties File

The following Identity Manager components use auditlogconfig.properties file to store the CEF configuration:

- Identity Vault
- Identity Manager Engine
- Java Remote Loader
- Fanout Agent

For information about the content of the audit properties file for each of these Identity Manager components, see the following sections:

- “Identity Manager Engine, Remote Loader, and .NET Remote Loader” on page 53
- “Java Remote Loader and Fanout Agent” on page 57

Identity Manager Engine, Remote Loader, and .NET Remote Loader

The following is a sample auditlogconfig.properties file for Identity Manager engine, Remote Loader, and .NET Remote Loader:

```plaintext
# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL)
#log4j.appender.S.Protocol=SSL

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem
```
# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=/var/opt/novell/eDirectory

# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
#log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n

NOTE: By default, the appenders are disabled. You need to manually enable them.

Before using the auditlogconfig.properties file, NetIQ recommends you to review the following considerations:

- The letters S and R specify Syslog Appender and Rolling File Appender respectively.
- Entries in the auditlogconfig.properties file are not case sensitive.
- Entries in the auditlogconfig.properties file can appear in any order.
- Empty lines in the file are valid.
- Any line that starts with a hash (#) is commented out.

The following table provides an explanation of each property in the auditlogconfig.properties file:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log4j.rootLogger</td>
<td>Sets the level of the root logger to debug and attaches an appender named R or S, where S specifies a Syslog appender and R specifies a Rolling File appender.</td>
</tr>
<tr>
<td>log4j.appender.S</td>
<td>Specifies the appender S to be a Syslog appender.</td>
</tr>
<tr>
<td>log4j.appender.S.Host</td>
<td>Specifies the location of the Syslog server where audit events are logged.</td>
</tr>
<tr>
<td>log4j.appender.S.Port</td>
<td>The port at which the Auditing server connects to the Syslog server. If the connection between Auditing server and the Syslog server fails, Identity Manager cannot log events until the connection is restored.</td>
</tr>
<tr>
<td>log4j.appender.S.Protocol</td>
<td>Specifies the protocol to use. For example, UDP, TCP, or SSL. SSL is the default protocol. For enabling secure communication, see Chapter 6, “Securing the Logging System,” on page 29.</td>
</tr>
<tr>
<td>log4j.appender.S.SSLCertFile</td>
<td>Specifies the SSL certificate file for the SSL connection. Use double backslashes to specify the path of the file. This is an optional setting.</td>
</tr>
<tr>
<td>log4j.appender.S.Threshold</td>
<td>Specifies the minimum log level allowed in the Syslog appender. INFO is the only supported log level.</td>
</tr>
<tr>
<td>log4j.appender.S.Facility</td>
<td>Specifies the type of facility.</td>
</tr>
<tr>
<td>log4j.appender.S.CacheEnabled</td>
<td>Specifies caching for Syslog appender.</td>
</tr>
<tr>
<td>log4j.appender.S.CacheDir</td>
<td>Specifies the directory for storing the cache file.</td>
</tr>
<tr>
<td>log4j.appender.S.CacheMaxFileSize</td>
<td>Specifies the size of the cache file. The range is 50 MB to 4000 MB.</td>
</tr>
<tr>
<td>log4j.appender.S.layout</td>
<td>Layout setting for Syslog appender.</td>
</tr>
<tr>
<td>log4j.appender.R</td>
<td>Specifies appender R to be a Rolling File appender.</td>
</tr>
<tr>
<td>log4j.appender.R.File</td>
<td>The location of the log file for a Rolling File appender.</td>
</tr>
<tr>
<td>log4j.appender.R.MaxFileSize</td>
<td>The maximum size, in MBs, of the log file for a Rolling File appender. Set this value to the maximum size that the client allows. This field accepts only integer value.</td>
</tr>
<tr>
<td>log4j.appender.R.MaxBackupIndex</td>
<td>Specify the maximum number of backup files for a Rolling File appender. The maximum number of the backup files can be 10. A zero value means no backup files.</td>
</tr>
<tr>
<td>log4j.appender.R.layout</td>
<td>Layout setting for Rolling File appender.</td>
</tr>
</tbody>
</table>
Enabling the Syslog Appender

1. Change the following entry to S to attach a Syslog appender:
   ```
   log4j.rootLogger=debug, S
   ```

2. Uncomment the following entries:
   ```
   log4j.appender.S=org.apache.log4j.net.SyslogAppender
   log4j.appender.S.Host=localhost
   log4j.appender.S.Port=port
   log4j.appender.S.Protocol=SSL
   log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem
   log4j.appender.S.Threshold=INFO
   log4j.appender.S.Facility=USER
   log4j.appender.S.layout=org.apache.log4j.PatternLayout
   log4j.appender.S.layout.ConversionPattern=%c: =%m%n
   ```

3. Log in to iManager and change the log events.
   For more information on changing log levels by using iManager, see “Setting the Log Level and Maximum Log Size” on page 37.


Enabling the Rolling File Appender

The Rolling File appender is preferred, if the auditing solution is limited to an individual server. Rolling file appender is more reliable compared to the Syslog appender because it uses the file connector to send events from your local file system to the auditing server.

1. Change the following entry to R to attach a Rolling File appender:
   ```
   log4j.rootLogger=debug, R
   ```

2. Uncomment the following entries:
   ```
   log4j.appender.R=org.apache.log4j.RollingFileAppender
   log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log
   log4j.appender.R.MaxFileSize=100MB
   log4j.appender.R.MaxBackupIndex=10
   log4j.appender.R.layout=org.apache.log4j.PatternLayout
   log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
   ```

3. Log in to iManager and change log levels.
   For more information on changing log levels by using iManager, see “Setting the Log Level and Maximum Log Size” on page 37.

Java Remote Loader and Fanout Agent

The following is a sample auditlogconfig.properties file for the Java Remote Loader and the Fanout agent.

```java
# Defines location of Syslog server.
#SyslogHost=localhost
#SyslogPort=port

# Specify protocol to be used (UDP/TCP/SSL)
#SyslogProtocol=TCP

# Specify SSL keystore file for SSL connection.
# File path should be given with double backslash.
#SyslogSSLKeystoreFile=/opt/netiq/idm/jre/lib/security/cacerts

# Specify SSL keystore password for SSL connection.
#SyslogSSLKeystorePassword=password

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#CacheDir=/tmp/IDMcache

# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#CacheRolloverSize=50

# Log file for appender
#FileAppenderFileName=/var/opt/novell/log/cef-events.log
```

The following table provides an explanation of each property in the auditlogconfig.properties file:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyslogHost</td>
<td>Specifies the location of the Syslog server where audit events are logged.</td>
</tr>
<tr>
<td>SyslogPort</td>
<td>The port at which the Auditing server connects to the Syslog server.</td>
</tr>
<tr>
<td></td>
<td>If the connection between Auditing server and the Syslog server fails, Identity Manager cannot log events until the connection is restored.</td>
</tr>
<tr>
<td>SyslogProtocol</td>
<td>Specifies the protocol to use. For example, UDP, TCP, or SSL.</td>
</tr>
<tr>
<td>SyslogSSLKeystoreFile</td>
<td>Specifies the SSL certificate file for the SSL connection. Use double backslashes to specify the path of the file. This is an optional setting.</td>
</tr>
<tr>
<td>SyslogSSLKeystorePassword</td>
<td>Specifies the keystore password for the SSL connection.</td>
</tr>
</tbody>
</table>
Understanding the Properties Files for CEF Auditing

The following is a sample of the `idmuserapp_logging.xml` file:

```xml
<logging xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="logging-config.xsd">

  <!-- example of enabling TRACE level -->
  <!--
  <logger name="com.novell.soa.af" additivity="true" level="TRACE"/>
  -->
  <!--
  <logger name="com.novell" additivity="true" level="INFO">
    <appender-ref ref="CONSOLE_DEBUG"/>
  </logger>
  -->

  <!-- Appender definitions -->
  <appenders>
    <!-- CONSOLE and FILE appender are defined in jboss-log4j.xml -->
    <!-- CEF appender -->
    <appender class="com.netiq.idm.logging.syslog.CEFSyslogAppender"
      name="CEF"/>

    <param name="Threshold" value="INFO"/>
    <param name="Facility" value="user"/>
    <param name="SyslogHost" value="${com.netiq.ism.audit.cef.host:localhost}"/>
    <param name="SyslogPort" value="${com.netiq.ism.audit.cef.port:1468}"/>
    <param name="SyslogProtocol" value="${com.netiq.ism.audit.cef.protocol:tcp}"/>
    <param name="SyslogSslKeystoreFile" value="${com.netiq.idm.audit.cef.tls-keystore:/opt/netiq/idm/apps/jre/lib/security/cacerts}"/>
    <param name="SyslogSslKeystorePassword" value="${com.netiq.idm.audit.cef.tls-keystore-password:KeystorePassword}"/>
    <param name="CacheDir" value="${com.netiq.ism.audit.cef.cache-enabled:yes}"/>
    <param name="CacheRolloverSize" value="${com.netiq.ism.audit.cef.cache-rollover-size:50 MB}"/>
    <param name="FileAppenderFileName" value="${com.netiq.idm.audit.cef.file-appender:log/audit.log}"/>
    <param name="AppendComponentName" value="yes"/>
  </appenders>

</logging>
```

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CacheEnabled</td>
<td>Specifies caching for SysLogAppender. The values can be yes or no.</td>
</tr>
<tr>
<td>CacheDir</td>
<td>Specifies the directory for storing the cache file.</td>
</tr>
<tr>
<td>CacheRolloverSize</td>
<td>Specifies the size of the cache file. The range is 50 MB to 4000 MB.</td>
</tr>
<tr>
<td>FileAppenderFileName</td>
<td>Specifies the log file for appender.</td>
</tr>
<tr>
<td>AppendComponentName</td>
<td>Specifies whether you want to append the component name before the event message. You can set this option to Yes if you are using Sentinel as your auditing solution.</td>
</tr>
</tbody>
</table>

Understanding the `idmuserapp_logging.xml` File

The following is a sample of the `idmuserapp_logging.xml` file:

```xml
<logging xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="logging-config.xsd">

  <!-- example of enabling TRACE level -->
  <!--
  <logger name="com.novell.soa.af" additivity="true" level="TRACE"/>
  -->
  <!--
  <logger name="com.novell" additivity="true" level="INFO">
    <appender-ref ref="CONSOLE_DEBUG"/>
  </logger>
  -->

  <!-- Appender definitions -->
  <appenders>
    <!-- CONSOLE and FILE appender are defined in jboss-log4j.xml -->
    <!-- CEF appender -->
    <appender class="com.netiq.idm.logging.syslog.CEFSyslogAppender"
      name="CEF"/>

    <param name="Threshold" value="INFO"/>
    <param name="Facility" value="user"/>
    <param name="SyslogHost" value="${com.netiq.ism.audit.cef.host:localhost}"/>
    <param name="SyslogPort" value="${com.netiq.ism.audit.cef.port:1468}"/>
    <param name="SyslogProtocol" value="${com.netiq.ism.audit.cef.protocol:tcp}"/>
    <param name="SyslogSslKeystoreFile" value="${com.netiq.idm.audit.cef.tls-keystore:/opt/netiq/idm/apps/jre/lib/security/cacerts}"/>
    <param name="SyslogSslKeystorePassword" value="${com.netiq.idm.audit.cef.tls-keystore-password:KeystorePassword}"/>
    <param name="CacheDir" value="${com.netiq.ism.audit.cef.cache-enabled:yes}"/>
    <param name="CacheRolloverSize" value="${com.netiq.ism.audit.cef.cache-rollover-size:50 MB}"/>
    <param name="FileAppenderFileName" value="${com.netiq.idm.audit.cef.file-appender:log/audit.log}"/>
    <param name="AppendComponentName" value="yes"/>
  </appenders>

</logging>
```
Understanding the Properties Files for CEF Auditing

```xml
<param name="CacheRolloverSize" value="2"/>
<param name="ApplicationName" value="RBPM"/>
<param name="EventPrefix" value="IDM:"/>
</appender>
</appenders>

<!--
Logger definitions

NOTE: CONSOLE & FILE appenders should be defined in (jboss-)
log4j.xml file.

Additivity of true means the loggers defined below will inherit the
appenders.
-->
<loggers>
  <logger name="com.novell" level="INFO" additivity="true">
    <appender-ref ref="CEF"/>
  </logger>
  <logger name="com.sssw" level="INFO" additivity="true">
    <appender-ref ref="CEF"/>
  </logger>
  <logger name="com.netiq" level="INFO" additivity="true">
    <appender-ref ref="CEF"/>
  </logger>
  <logger name="com.novell.afw.portal.aggregation" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.portal.persist" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.portal.portlet" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.portal.util" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.portal.portlet.consumer" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.portal.portlet.core" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.portal.persist" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.portal.producer" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.portal.util" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.theme" level="INFO" additivity="true"/>
  <logger name="com.novell.afw.util" level="INFO" additivity="true"/>
  <logger name="com.novell.common.auth" level="INFO" additivity="true"/>
  <logger name="com.novell.idm.security.authorization.service" level="INFO" additivity="true"/>
  <logger name="com.novell.pwmdmgt.actions" level="INFO" additivity="true"/>
  <logger name="com.novell.pwmdmgt.util" level="INFO" additivity="true"/>
  <logger name="com.novell.pwmdmgt.service" level="INFO" additivity="true"/>
</loggers>
```
Understanding the workflow_logging.xml File

The following is a sample of the workflow_logging.xml file:

```xml
<logging xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="logging-config.xsd">
  <prefix>[WORKFLOW]</prefix>
  <!-- example of enabling TRACE level -->
  <!--
  <logger name="com.novell.soa.af" additivity="true" level="TRACE"/>
  -->
  <!--
  <logger name="com.novell" additivity="true" level="INFO">
    <appender-ref ref="CONSOLE_DEBUG"/>
  </logger>
  -->
  <!-- Appender definitions -->
  <appenders>
    <!-- CONSOLE and FILE appender are defined in jboss-log4j.xml -->
    <!-- CEF appender -->
    <appender class="com.netiq.idm.logging.syslog.CEFSyslogAppender" name="WFCEF">
      <param name="Threshold" value="INFO"/>
      <param name="Facility" value="user"/>
      <param name="SyslogHost" value="${com.netiq.ism.audit.cef.host=localhost}" />
      <param name="SyslogPort" value="${com.netiq.ism.audit.cef.port=1468}" />
      <param name="SyslogProtocol" value="${com.netiq.ism.audit.cef.protocol=tcp}" />
      <param name="SyslogSslKeystoreFile" value="${com.netiq.idm.audit.cef.tls-keystore:/opt/netiq/idm/apps/jre/lib/security/cacerts}" />
      <param name="SyslogSslKeystorePassword" value="${com.netiq.idm.audit.cef.tls-keystore-password:KeystorePassword}" />
    </appender>
  </appenders>
</logging>
```
<param name="CacheDir" value="${com.netiq.ism.audit.cef.cache-file-dir:/opt/netiq/idm/apps}" />
<param name="CacheRolloverSize" value="2"/>
<param name="ApplicationName" value="WORKFLOW"/>
<param name="EventPrefix" value="IDM:"/>
</appender>
</appenders>

<!-- Logger definitions
NOTE: CONSOLE & FILE appenders should be defined in (jboss-)log4j.xml file.
Additivity of true means the loggers defined below will inherit the appenders.
-->
<loggers>
  <logger name="workflow.log" level="INFO" additivity="true">
   <appender-ref ref="WFCEF"/>
  </logger>
  <logger name="com.novell" level="INFO" additivity="true">
   <appender-ref ref="WFCEF"/>
  </logger>
  <logger name="com.netiq" level="INFO" additivity="true">
   <appender-ref ref="WFCEF"/>
  </logger>
  <logger name="com.sssw" level="INFO" additivity="true">
   <appender-ref ref="WFCEF"/>
  </logger>
  <logger name="com.microfocus" level="INFO" additivity="true">
   <appender-ref ref="WFCEF"/>
  </logger>
</loggers>
<root>
  <priority value="INFO"/>
</root>
</logging>

Understanding the idmrptdcs_logging.xml File

The following is a sample of the idmrptdcs_logging.xml file:
<logging>
</logging>

<!-- Prefix for logging messages from this logger configuration -->
<prefix>[DCS-CORE]</prefix>

<loggers>
  <logger additivity="true" name="com.novell" level="INFO">
  </logger>
  <logger additivity="true" name="com.netiq" level="INFO">
  </logger>
</loggers>

<audit>
<!-- Defines location of Syslog server. -->
<!--
<SyslogHost>127.0.0.1</SyslogHost>
<SyslogPort>1468</SyslogPort>
-->
<!-- Specify protocol to be used (UDP/TCP/SSL) -->
<!--
<SyslogProtocol>TCP</SyslogProtocol>
-->

<!-- Specify SSL keystore file for SSL connection. -->
~ File path should be given with double backslash.
<!--
<SyslogSSLKeystoreFile>/etc/opt/novell/mycert.pem</SyslogSSLKeystoreFile>
-->
<!-- For Linux -->
<!--
<SyslogSSLKeystoreFile>/etc/opt/novell/mycert.pem</SyslogSSLKeystoreFile>
-->
<!-- For Windows, file path should be given with double backslash. -->
<!--
<SyslogSSLKeystoreFile>C:\Novell\mycert.pem</SyslogSSLKeystoreFile>
-->
<!-- Specify SSL keystore password for SSL connection. -->
<!--
<SyslogSSLKeystorePassword>password</SyslogSSLKeystorePassword>
-->

<!-- Specify whether to append the component name before the event message -->
~ Inputs should be yes/no
~ If NetIQ Sentinel is the event listener, this option should be set to 'yes'
<!--
<AppendComponentName>yes</AppendComponentName>
-->

<!-- Defines caching for SyslogAppender. -->
~ Inputs should be yes/no
<!--
<CacheEnabled>yes</CacheEnabled>
-->
<!--Cache location Directory
~ Directory should be available for creating cache files
~ Directory should have 'novlua' permission for caching to work correctly
-->
<!--For Linux-->  
<!--  
<CacheDir>/var/opt/netiq/idm/dcs-cache</CacheDir>
-->  
<!--For Windows, file path should be given with double backslash.-->  
<!--  
<CacheDir>C:\NetIQ\idm\IDMcache</CacheDir>
-->  

<!--Cache File Size
~ Cache File size should be in the range of 50MB to 4000MB
-->  
<!--  
<CacheRolloverSize>50</CacheRolloverSize>
-->  

<!--Log file for appender
~ The directory containing the file specified should have 'novlua' permission to work correctly.
-->  
<!--For Linux-->  
<!--  
<FileAppenderFileName>/var/opt/netiq/idm/dcs-cache/cef-events.log</FileAppenderFileName>
-->  
<!--For Windows, file path should be given with double backslash.-->  
<!--  
<FileAppenderFileName>C:\cef-events.log</FileAppenderFileName>
-->  

<!--Max size of log file for file appender -->  
<!--  
<FileMaxRolloverSize>50</FileMaxRolloverSize>
-->  
</audit>
</logging>

NOTE: By default, the appenders are disabled. You need to manually enable them by uncommenting the appender section.

Understanding the idmrptcore_logging.xml File

The following is a sample of the idmrptcore_logging.xml file:
<logging xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="logging-config.xsd">

<!-- Prefix for logging messages from this logger configuration -->
<prefix>[RPT-CORE]</prefix>

<audit>
  <syslog>
    <enabled>${com.netiq.ism.audit.cef.enabled:false}</enabled>
    <protocol>${com.netiq.ism.audit.cef.protocol:TCP}</protocol>
    <host>${com.netiq.ism.audit.cef.host:localhost}</host>
    <port>${com.netiq.ism.audit.cef.port:514}</port>
    <cache-dir>${com.netiq.ism.audit.cef.cache-file-dir:/tmp/rpt-syslog-cache}</cache-dir>
    <cache-file>idm-rpt</cache-file>
    <application>Identity Manager Reporting</application>
    <vendor>Micro Focus</vendor>
    <version>6.5.0</version>
    <keystore-file>${com.netiq.idm.osp.ssl-keystore.file:/tmp/keystore.jks}</keystore-file>
    <keystore-password>${com.netiq.idm.osp.ssl-keystore.pwd:changeit}</keystore-password>
    <keystore-type>${com.netiq.idm.osp.ssl-keystore.type:JKS}</keystore-type>
  </syslog>
</audit>

<!-- Logger definitions -->
<loggers>
  <!-- Example of enabling TRACE level -->
  <!--
  <logger additivity="true" name="com.novell.soa.af" level="TRACE"/>
  -->
  <logger additivity="true" name="com.novell" level="INFO"/>
  <logger additivity="true" name="com.netiq" level="INFO"/>
</loggers>
</logging>
Troubleshooting

This section provides useful information for troubleshooting problems with CEF Auditing.

Error on Identity Manager Dashboard Login Page

During the audit configuration, if the novlua permissions are not set for the Intermediate event store directory, then you will see the following error on login page of Identity Manager Dashboard.

{"Fault":{"Code":{"Value":"Sender","Subcode":{"Value":"XDAS_OUT_FAILURE"}},"Reason":{"Text":"System not in a fully started state. (perhaps starting, shutting down, refreshing configuration, or restarting)"}}}

Perform the following actions to resolve this error:

1. Change the permission of the intermediate event store directory by running the commands:
   ```
   chown novlua:novlua <directory_path>
   chmod 755 <directory_path>
   ```
   where `<directory_path>` is path to the intermediate event store directory.

2. Restart the Tomcat service.

3. Disable the CEF audit configuration using configuration update utility and restart the tomcat service. Now carefully repeat the configuration steps to enable CEF auditing.